REMARKS/ARGUMENTS

Claims 1-28 remain in this application for further review. The claims have not been amended in this response. No new matter has been added.

I. Interview of December 1, 2005

This application was filed on April 27, 2001 with a priority date of February 16, 2001. A Request for Continued Examination was filed on April 26, 2005. The Final Office Action referenced herein purports a new rejection that cites new art. Applicants' attorney held a brief interview with Examiner Henning on December 1, 2005. Examiner Henning suggested that if amendments to the claims are made, an RCE should be filed. Applicants' attorney explained that applicants' believe that the claims, as submitted herein, distinguish the references. Examiner Henning recommended that any explanations of the prior art and present invention be set forth in an Amendment After Final. Applicants hope that the Remarks herein clarify the prior art and result in allowance of the claims.

II. Rejection of Claims 1-28 Under 35 U.S.C. 103(a)

Claims 1-28 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,301,484 issued to Rogers et al. ("Rogers") in view of U.S. Patent No. 6,148,342 issued to Ho. ("Ho"). Applicants respectfully disagree with the Office Action. Even if the above references could be combined for argument sake, they still fail to teach all the limitations of the claims.

A. Claim Elements Not Taught by the References

Applicants' claim 1 specifically recites the following combination of elements that are not taught or suggested by the references:

> "identifying ***the source of the received message*** from data associated with the received message"
>
> "associating a security role ***with the received message*** based on the identified source of the received message"
>
> "inserting an identifier ***into the received message*** to identify the associated security role"
>
> "comparing the associated security role ***of the received message*** with a security privilege associated with the at least one configuration setting on the mobile device"

The specification of the present invention includes several examples. These examples are not referenced herein to limit the claims in any manner. The examples are referenced herein to help explain a few aspects of the present invention for the Examiner in hopes of bolstering applicants contentions below with regard to the references. The specification recites one example as follows:

> To begin, at block 703 a configuration message is received. The configuration message identifies its source and certain configuration transactions to be performed. At block 705, a security role is assigned to the message based on the source of the message...The security role assigned to the message corresponds to security credentials that have been pre-selected for the source of the message. At block 707, the message (including security role) is passes to an application registered to handle the configuration transaction.
>
> ...At block 711, a verification is performed to determine if the security role of the message is sufficient to invoke the identified CSP...If the security role of the message is insufficient, the transaction fails at block 714 and the configuration transaction is rolled back by returning any changed settings to their previous values. If the security role of the message is sufficient, the responsible CSP is invoked and passed the configuration message at block 715...
>
> At block 717, a verification is performed to determine if the security role of the message is sufficient to access the affected settings. As mentioned, each setting

> or group of settings has its own security role. If the security role of the message is insufficient, the transaction fails at block 714 and the configuration transaction is rolled back. However, if the security role of the message is sufficient, the CSP performs the requested configuration transaction at block 721. The process then ends at block 723. *Specification*, at page 15, line 20 - page 16, line 19.

The unique combination of elements recited above in claim 1 is not taught or otherwise suggest by the cited references. More specifically, neither of the references teach the elements of claim 1 in combination with ***a received message***. The Office Action purports that Rogers teaches "identifying the source of the received message from data associated with the received message." *See Office Action*, at page 2, lines 25-26. To support this proposition, the Office Action cites to column 4 of Rogers. This portion of Rogers recites as follows:

> "Each of the data fields may be encrypted in order to provide a level of security to the feature message. Alternatively, a data field consisting of encrypted authentication data may be used to provide message security." *Rogers*, at col. 4, lines 13-17.

A further read of the specification indicates that Rogers is teaching that the data fields may be encrypted when the message ***is sent (i.e before it is received by a device)***. Roger does not teach "identifying the source of the received message from data associated with the ***received message***." Succinctly stated, Rogers does not teach any type of security role assignment associated with ***a received message***.

The Office Action continues by conceding that Rogers fails to teach:

> "associating a security role with the received message based on the identified source of the received message; inserting an identifier into the received message to identify the associated security role; comparing the associated security role of the received message with a security privilege associated with the at least one configuration setting on the mobile device; and if the associated security role of the received message is in agreement with the security privilege associated with the at least one configuration setting on the mobile device, processing the request associated with the configuration information." *Office Action*, at page 3, lines 3-12.

The Office Action then propounds that Ho remedies this lack of teaching. However, Ho does not teach these elements. Ho pertains to a network having several terminals and databases. Similar to Rogers, Ho fails to teach the elements of claim 1 with respect to ***a received message***. Ho does not teach "associating a security role ***with the received message*** based on the identified source of the received message." Ho teaches as follows:

> "In block 204, a user at a source terminal requests data. The user may enter information such as a password, or other identifying information ***to indicate that the user*** is the entity he or she claims to be. ***The source terminal encrypts*** the subject's identifying information such as the patient name with a first code in block 208." *Ho*, at col. 5, lines 54-59.

Here, Ho clearly teaches that ***the source terminal*** encrypts the message. Ho also teaches that the identifying information is to indicate ***the user***. There is no teaching or suggestion of "associating a security role ***with the received message*** based on the ***identified source of the received message***." Moreover, Ho does not teach "inserting an identifier ***into the received message*** to identify the associated security role." Ho teaches as follows:

> If the doctor and patient are a doctor-patent pair, then access is allowed in decision block 230 and the database retrieves the (1) appropriate privilege level corresponding to the doctor-patient pair and (2) the internal ID corresponding to the patient in block 236. *Ho*, at col. 6, lines 33-36.

Ho is teaching that a privilege level is retrieved from a database in a distributed system. Such a process is clearly not the same as "associating a security role ***with the received message*** based on the ***identified source of the received message***." Ho teaches a distributed system that includes transmitting messages, identifications and data between several databases and terminals. However, the claim 1 specifically recites "***a configuration message.***" Claim 1 continues by reciting several elements that pertain to "***the*** configuration message." The requests, transmissions of identifications, and transmissions of client files described in Ho cannot be

analogized to the message recited above in claims 1. To do so would fail to consider that prior art and the claims of the invention as a whole. Accordingly, applicants assert that claim 1 is allowable over the cited references.

Applicants' claim 8 specifically recites the following elements that are not taught or suggested by the references:

> "a router configured to receive ***a configuration message*** over a wireless communication link, the router being further configured to identify ***a source of the configuration message*** and ***insert a security role identifier into the received configuration message based on the identified source***, the router being further configured to ***pass the configuration message*** to other components of the mobile device, the configuration message including an instruction that affects a configuration setting"

Applicants' claim 13 specifically recites the following elements that are not taught or suggested by the references:

> "receiving a configuration message ***including a header*** and an instruction associated with a configuration setting stored on the mobile device"
>
> "***identifying the source of the received message from the header of the received configuration message***"
>
> "associating a security role with the instruction based on the source ***of the received message***, wherein the associated security role is associated to the instruction by a tag included in the message"

Applicants' claim 20 specifically recites the following elements that are not taught or suggested by the references:

> "***a second field including a security role identifier***, wherein the security role identifier is ***configured for association with a configuration message***"
>
> "a third field including a security role associated with the configuration service provider, wherein, the security role of the configuration service provider identifies a provider privilege which must be had in order to make use of the configuration service provider, ***and wherein the third field is configured to determine when***

the security role identifier matches the security role of the configuration service provider"

Regarding independent claims 8, 13 and 20 applicants rely on the support provided above for claim 1. Regarding the dependent claims, claims 2-7, 9-12, 14-19 and 21-28 include elements not taught or otherwise suggested by the cited references. Also, claims 2-7, 9-12, 14-19 and 21-28 ultimately depend from independent claims 8, 13, and 20, respectively. Claims 8, 13, and 20 are thought allowable as stated above. Accordingly, applicants believe that claims 2-7, 9-12, 14-19 and 21-28 are allowable for at least those same reasons.

B. No Suggestion to Combine References as Propounded.

There is no suggestion in either of the references to combine them in the manner propounded. Rogers pertains to configuring a phone with an SMS message. Rogers specifically teaches as follows:

> "When a phone receives any SMS message, it must check to see if it is a feature control message. The phone performs this by performing the feature control routine of FIGS. 1A-1B. Referring to FIG. 1A, when an SMS message is received, the phone begins by comparing the first characters of the received message with a predetermined start of control message delimiter, step 104. To prevent the phone from falsely concluding that a received SMS message is a "feature control message" the "start of control" message delimiter is defined to be a series of characters that normally does not occur at the start of a message and that does not normally occur in sequence. As examples, the start of control message delimiter could be "??QC?", ((QC", or "))12". The number of characters and specific characters used are not limited but should be chosen to minimize false indications of feature control messages. If at step 104 it is determined that the first characters do not indicate a feature control message, the phone does not attempt to alter any features and merely handles the message as a normal SMS message, step 106." *Rogers*, at col. 5, lines 14-32.

Roger pertains to remotely configuring a phone with a message via a cellular network. Ho does not relate to such an art. Ho pertains to a obtaining access to files and other data in a distributed network of terminals where date, identifications and requests are transmitted between several terminals and databases. A person, such as Rogers, concerned with wireless cellular telephone technology and messages for configuring the same, would not be inclined to consider a reference that teaches authentication in a distributed system. Both Roger and Ho teach systems to accomplish very different goals that are unrelated to each other. Accordingly, applicants assert that Rogers cannot be modified as propounded.

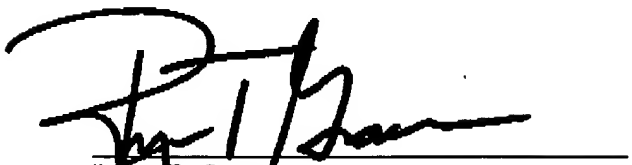
III. Request For Reconsideration

In view of the foregoing amendments and remarks, all pending claims are believed to be allowable and the application is in condition for allowance. Therefore, a Notice of Allowance is respectfully requested. Should the Examiner have any further issues regarding this application, the Examiner is requested to contact the undersigned attorney for the applicants at the telephone number provided below.

App. No. 09/843,901
Amendment Dated December 6, 2005
Reply to Office Action of November 2, 2005

Respectfully submitted,

MERCHANT & GOULD P.C.



Ryan T. Grace
Registration No. 52,956
Direct Dial: 206.342.6258

MERCHANT & GOULD P.C.
P. O. Box 2903
Minneapolis, Minnesota 55402-0903
206.342.6200